


Summary

This guide outlines the process of decrypting files encrypted by Phobos/8base ransomware. The characteristic of the decrypted files that this tool supports decryption of are as follow;

- Example of encrypted file name

 `example.txt.id[B01E7FEA-0001].[mail@example.com].phobos`

- ※ Naming rule

{Original Filename} .id[{8 random characters}-{4 digit numbers}].[{Mail address}].[File Extensions]

- Examples of encrypted file extension

.phobos .8base .elbie .faust .LIZARD

- ※ In addition to the above file extensions, several other file extensions have been identified. If the file name matches the above example, it may be decrypted by this tool.

(Note)

- Even in cases encrypted by Phobos/8base ransomware, in cases where the decrypted files are corrupted due to encryption failure or a bug in encryption process, it cannot be decrypted.
- This tool doesn't guarantee the integrity of the decrypted files.



警察庁
National Police Agency



How to Use the Decryption tool

Step1 Download and Run the Decryption tool

- Download the "PhDec Decryptor" from NO MORE RANSOM (<https://www.nomoreransom.org>)
- Run the "Phdec_gui_v***.exe" execution file.

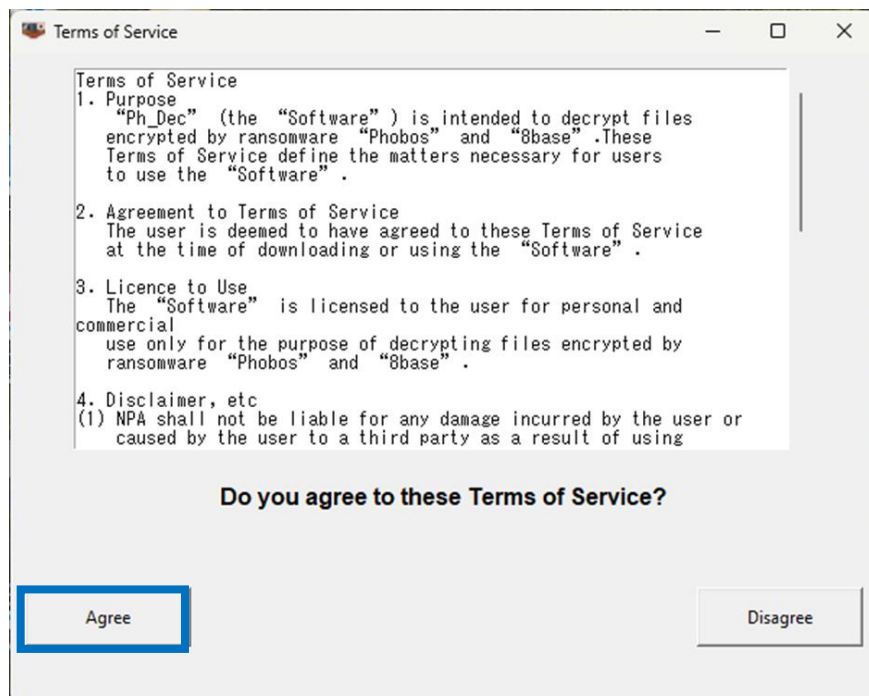


(Caution)

- This tool may be mis-detected by anti-virus software.

Step2 Agree to Terms of Service

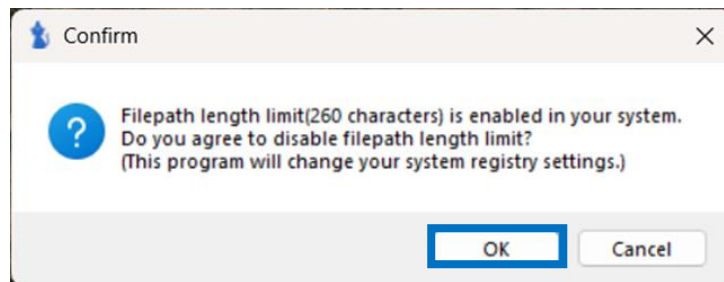
Please read the Terms of Service. If you agree, press the [Agree] button.



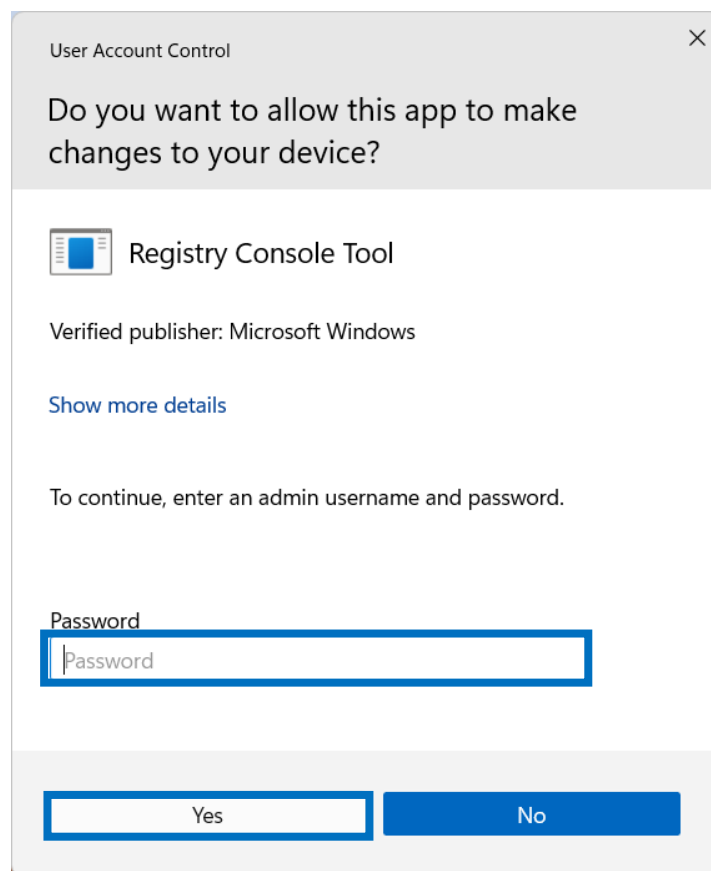
警察庁
National Police Agency



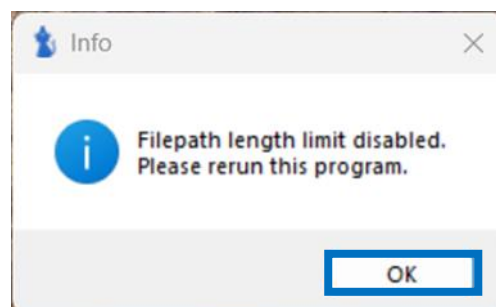
If the following dialog is displayed, press [OK] button.



If the following dialog is displayed, input your password and press [Yes] button.



If the following dialog is displayed, press [OK] button and re-run the tool.



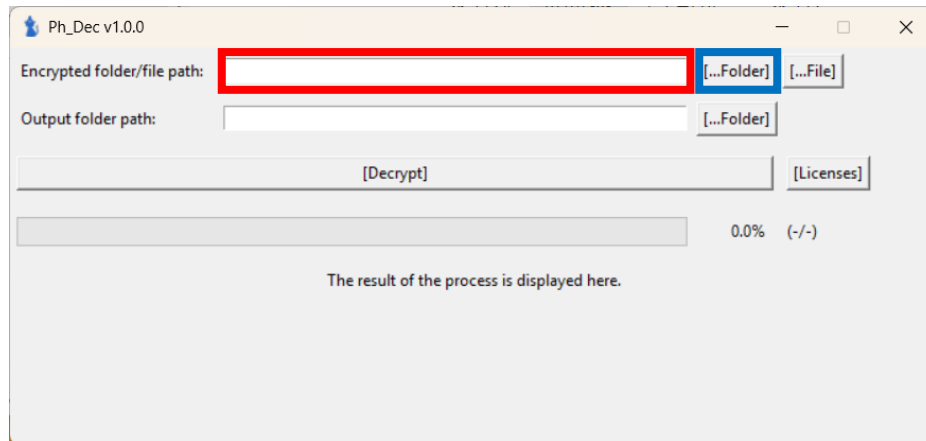
警察庁
National Police Agency



Step3 Select full path of target folder/file.

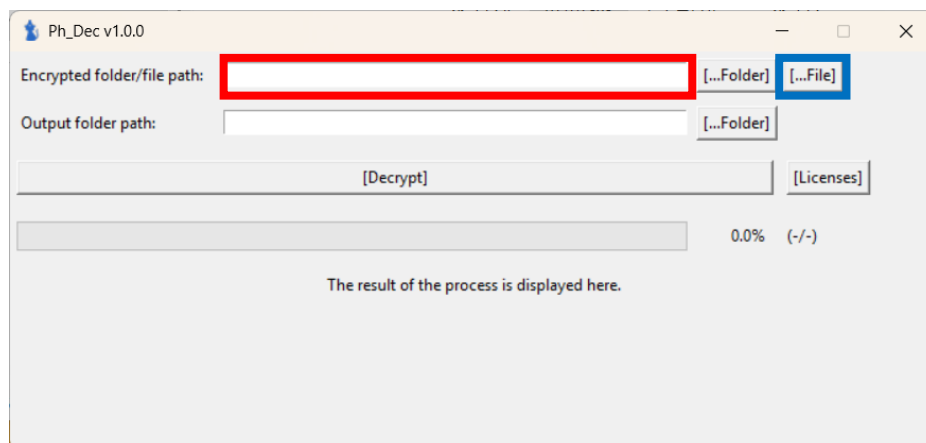
Step3-1 When the target is the folder

- Attempts to decrypt all files in the folder and subfolder.
- Press the [...Folder] button and select target folder or drag and drop the target folder onto the red square.



Step3-2 When the target is the file

- Attempts to decrypt only selected file.
- Press the [...File] button and select target file or drag and drop the target folder onto the red square.

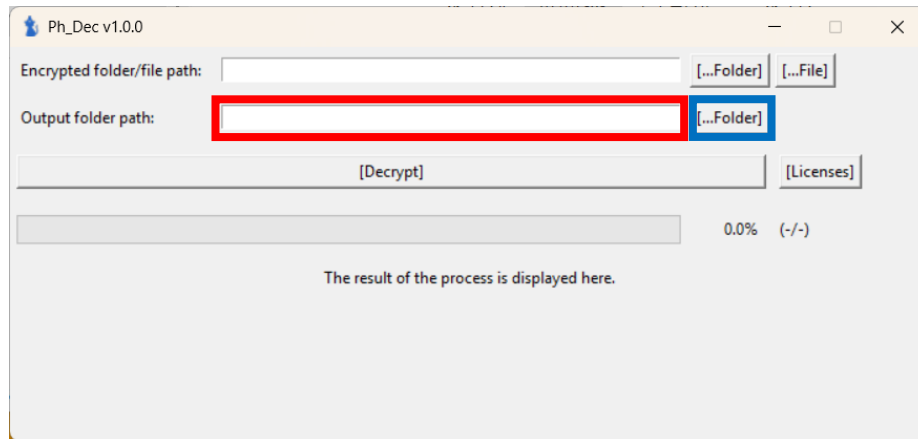


警察庁
National Police Agency



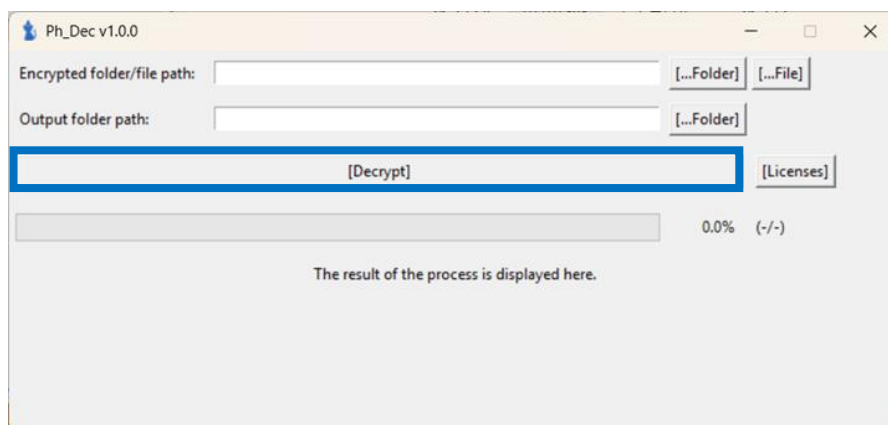
Step4 Select Output folder full path

Press the [...Folder] button and select output folder or drag and drop the target folder onto the red square.



Step5 Start Decryption

Press the [Decrypt] button and start decryption process.



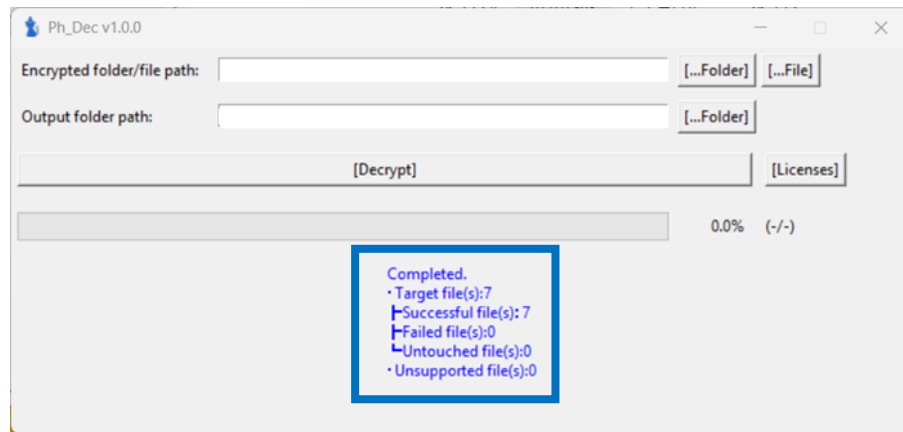
警察庁
National Police Agency



Step6 Complete Decryption

When the decryption process is complete, the message dialog "Completed." is displayed.

The decrypted files have created in the output specified in "Step 4".



- Target file(s): Number of target files.
 - Successful file(s): Number of successfully decrypted files.
 - Failed file(s): Number of files that failed to decrypt.
 - Untouched file(s): Number of unprocessed files.
- Unsupported file(s): Number of excluded files (file corruption, etc.).

Reference

This tool will output the decryption results to "output_{Date}.txt" , "output_{Date}.csv" and "error.log".

"output.csv" is created in [log] folder inside the tool folder.

"output.csv" has items [filepath] and [decrypted].

Item [decrypted] records the decryption result of each file as follows:

[yes] : Decryption success

[no] : Decryption failed (Details are recorded in the log)

[no_keys] : encrypted key broken

[corrupted] : File corruption or Incomplete encryption



警察庁
National Police Agency

